AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for enabling a database system to prove that an origin system sent a message, comprising:

receiving the message and a signed first digest of the message at a database system from the origin system, wherein the signed first digest was created by signing a digest of the message using an origin private encryption key;

using an origin public encryption key that is associated with the origin private encryption key to verify that the signed first digest was signed by the origin system, thereby proving that the origin system created and sent the message; and

persistently storing the signed first digest with the message, ~~thereby~~ which ~~enabling~~ enables the database system to present the signed first digest as proof that the origin system sent the message, thereby preventing the sender from persuasively denying that the sender sent the message.

2. (Canceled).

3. (Previously presented) The method of claim 22, further comprising passing the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

4. (Original) The method of claim 3, further comprising passing the message and the digest through a plurality of databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

5. (Previously presented) The method of claim 1, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

6. (Previously presented) The method of claim 22, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

7. (Previously presented) The method of claim 1, wherein computing the digest includes using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

8. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for enabling a database system to prove that an origin system sent a message, the method comprising:

receiving the message and a signed first digest of the message at a database system from the origin system, wherein the signed first digest was created by signing a digest of the message using an origin private encryption key;

using an origin public encryption key that is associated with the origin private encryption key to verify that the signed first digest was signed by the origin system, thereby proving that the origin system created and sent the message; and persistently storing the signed first digest with the message, ~~thereby~~ which ~~enabling~~ enables the database system to present the signed first digest as proof that the origin system sent the message, thereby preventing the sender from persuasively denying that the sender sent the message.

9. (Canceled).

10. (Previously presented) The computer-readable storage medium of claim 23, the method further comprising passing the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

11. (Original) The computer-readable storage medium of claim 10, the method further comprising passing the message and the digest through a plurality of databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

12. (Previously presented) The computer-readable storage medium of claim 8, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

13. (Previously presented) The computer-readable storage medium of claim 23, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

14. (Previously presented) The computer-readable storage medium of claim 8, wherein computing the digest includes using one of message digest 2

(MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

15. (Currently amended) An apparatus for enabling a database system to prove that an origin system sent a message, comprising:

a first receiving mechanism that is configured to receive the message and a signed first digest of the message at a database system from the origin system, wherein the signed first digest was created by signing a digest of the message using an origin private encryption key;

a first verifying mechanism that is configured to use an origin public encryption key that is associated with the origin private encryption key to verify that the signed first digest was signed by the origin system, thereby proving that the origin system created and sent the message; and

a first storing mechanism that is configured to persistently store the signed first digest with the message, ~~thereby~~ which ~~enabling~~ enables the database system to present the signed first digest as proof that the origin system sent the message, thereby preventing the sender from persuasively denying that the sender sent the message.

16. (Canceled).

17. (Previously presented) The apparatus of claim 24, further comprising a passing mechanism that is configured to pass the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

18. (Original) The apparatus of claim 17, wherein the passing mechanism is further configured to pass the message and the digest through a plurality of

databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

19. (Previously presented) The apparatus of claim 15, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

20. (Previously presented) The apparatus of claim 24, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

21. (Previously presented) The apparatus of claim 15, wherein computing the digest includes using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

22. (Previously presented) The method of claim 1, further comprising:

receiving a signed receive-request from a recipient system for receiving the message, wherein the receive-request is signed using a recipient private encryption key;

validating the signed receive-request using a recipient public encryption key that is associated with the recipient private encryption key;

sending a second digest of the message to the recipient system;

receiving a signed second digest from the recipient system, wherein the signed second digest was created by signing the second digest using the recipient private encryption key;

validating the signed second digest using the recipient public encryption key, thereby proving that the recipient system requested to receive the message; and

persistently storing the signed second digest, thereby enabling the database system to present the signed second digest as proof that the recipient system requested to receive the message.

23. (Previously presented) The computer-readable storage medium of claim 8, the method further comprising:

receiving a signed receive-request from a recipient system for receiving the message, wherein the receive-request is signed using a recipient private encryption key;

validating the signed receive-request using a recipient public encryption key that is associated with the recipient private encryption key;

sending a second digest of the message to the recipient system;

receiving a signed second digest from the recipient system, wherein the signed second digest was created by signing the second digest using the recipient private encryption key;

validating the signed second digest using the recipient public encryption key, thereby proving that the recipient system requested to receive the message; and

persistently storing the signed second digest, thereby enabling the database system to present the signed second digest as proof that the recipient system requested to receive the message.

24. (Previously presented) The apparatus of claim 15, further comprising:

a second receiving mechanism configured to receive a signed receive-request from a recipient system for receiving the message, wherein the receive-request is signed using a recipient private encryption key;

a second validating mechanism configured to validate the signed receive-request using a recipient public encryption key that is associated with the recipient private encryption key;

a second sending mechanism configured to send a second digest of the message to the recipient system;

a third receiving mechanism configured to receive a signed second digest from the recipient system, wherein the signed second digest was created by signing the second digest using the recipient private encryption key;

a third validating mechanism configured to validate the signed second digest using the recipient public encryption key, thereby proving that the recipient system requested to receive the message; and

a second storing mechanism configured to persistently store the signed second digest, thereby enabling the database system to present the signed second digest as proof that the recipient system requested to receive the message.